WEST Search History

DATE: Monday, September 29, 2003

Set Name side by side	Query	Hit Count	Set Name result set
	DB=USPT; PLUR=YES; OP=OR		
L12	L11 and l4	1	L12
L11	L10 same l1	2	L11
L10	L9 same l8	56	L10
L9	initial near5 seed	1824	L9
L8	group$	1008825	L8
L7	L6 and l5	19	L7
L6	(128 or 256 or 512 or 1024 or 2048) near7 bit	32127	L6
L5	L4 and l3	105	L5
L4	@ad<19970715	2510314	L4
L3	L2 same l1	201	L3
L2	(new or different) near7 seed	6489	L2
L1	random$ near7 number	24225	L1

END OF SEARCH HISTORY

WEST

Generate Collection | Print

L7: Entry 8 of 19 File: USPT May 16, 1995

DOCUMENT-IDENTIFIER: US 5416783 A
TITLE: Method and apparatus for generating pseudorandom numbers or for performing data compression in a data processor

Application Filing Date (1):
19930809

Detailed Description Text (39):
The manner in which the pseudo-random numbers, and thus the pseudo-random bits, are generated will now be discussed. Referring to FIG. 5, flattened oval 306 indicates the point in the flow diagram where the generation of pseudo-random numbers is started. Rectangles 360-362 illustrate data movement steps which properly initialize CPU 20 so that pseudo-random numbers can be generated. A SEED value and a MASK value are received by arithmetic logic unit (ALU) 152. The SEED value and the MASK value are used to generate a pseudo-random number which is then used as a "NEW SEED" value to generate the next pseudo-random number (see rectangle 364 in FIG. 5).

Detailed Description Text (41):
The binary numbers in TABLE 1 are included as an illustrative example of how each step is performed. The SEED values, including old SEED and NEW SEED represent individual numbers in a sequence of pseudo-random numbers.

Detailed Description Text (68):
Test control circuitry 120 controls the loading of down counter 128 by way of load signal 130. If the most significant bit place of the MASK value which stores a logical one is the "Nth" bit, then the value "N" is loaded into down counter 128. For example, if the most significant bit place of the MASK value which stores a logical one is the "14th" bit, then the value "14" is loaded into down counter 128. Down counter is then decremented (see rectangle 386 in FIG. 7) until down counter 128 reaches a zero value. When down counter 128 reaches a zero value, down counter 128 asserts a zero count signal 126. Note that alternate embodiments of the present invention may use an up counter with match circuitry (not shown) instead of down counter 128.

Detailed Description Text (99):
In one embodiment of the present invention illustrated in FIG. 3, all of the circuitry but the scan-input latches 154, the scan-output latches 158, the down counter 128, the DONE bit 124, conductor 157, D-bus 113, logical ANDing circuit 140, replicating circuit 138, test signal 32, and test control logic 120 were already being used by CPU 20 for other functions in a normal operating mode which were unrelated to the present invention. Thus by adding a relatively small amount of circuitry, CPU 20 was now able to perform BIST scan testing, which included the generation of pseudo-random numbers and the performance of data compression.

WEST

Generate Collection | Print

L7: Entry 9 of 19 File: USPT Sep 1, 1992

DOCUMENT-IDENTIFIER: US 5144667 A
TITLE: Method of secure remote access

Application Filing Date (1):
19901220

Detailed Description Text (11):
To assure difficulty of deriving F or B, it is preferred that they have a length of several hundred bits, although a practical system may have only about 256 bits. While the base unit 12 may have a random number generator, this is not desirable for the remote unit 14. To provide such a large number F, having a random nature, a small random or pseudo-random seed number is provided by the base unit and passed to the remote unit. This seed is operated upon in conjunction with the secret key S to generate a number having 256 bits which is used as the exponent F.

Detailed Description Text (21):
It is not necessary to include a random number generator in the IC. For the base unit a host computer can perform this function in software. The remote unit does not need its own random numbers. During sign-up the remote unit needs a seed number which is different each time. As described above, a different number is provided by the base unit and the remote unit makes it secret by encrypting it with the secret key S. The number is both unpredictable and secret without an explicit random number generator.